ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

ДЕПАРТАМЕНТ ИМУЩЕСТВЕННЫХ И ЗЕМЕЛЬНЫХ ОТНОШЕНИЙ КУРГАНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 8 августа 2017 года № 42
г. Курган

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки в Департаменте имущественных и земельных отношений Курганской области и подведомственных Департаменту имущественных и земельных отношений Курганской области государственных предприятиях

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152 - ФЗ «О персональных данных»

ПОСТАНОВЛЯЕТ:

1. Определить перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки в Департаменте имущественных и земельных отношений Курганской области (далее — Департамент) и подведомственных Департаменту государственных предприятиях (далее — Перечень) согласно приложению 1 к настоящему постановлению.

2. Департаменту и подведомственным Департаменту государственным предприятиям при разработке частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных адаптировать Перечень руководствуясь приложением 2 к настоящему постановлению.

3. Опубликовать настоящее постановление в установленном порядке.

4. Контроль за исполнением настоящего постановления возложить на заместителя директора Департамента имущественных и земельных отношений Курганской области — начальника управления доходов и организационной работы.

Директор Департамента имущественных и земельных отношений Курганской области М.Ю. Герштанский

Лепшина Е.М.,
(3522) 46-18-73

Приложение 1 к постановлению
Департамента имущественных и
земельных отношений Курганской области
от 8 августа 2017 года № 42
«Об определении угроз безопасности
персональных данных, актуальных при
обработке персональных данных в
информационных системах персональных
данных, эксплуатируемых при
осуществлении соответствующих видов
деятельности, с учетом содержания
персональных данных, характера и
способов их обработки в Департаменте
имущественных и земельных отношений
Курганской области и подведомственных
Департаменту имущественных и
земельных отношений Курганской области
государственных предприятиях»

Перечень
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки в Департаменте имущественных и земельных отношений Курганской области и подведомственных Департаменту имущественных и земельных отношений Курганской области государственных предприятиях

Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю Российской Федерации

1. Угроза внедрения кода или данных.
2. Угроза воздействия на программы с высокими привилегиями.
3. Угроза восстановления аутентификационной информации.
4. Угроза выхода процесса за пределы виртуальной машины.
5. Угроза доступа к защищаемым файлам с использованием обходного пути.
6. Угроза доступа/перехвата/изменения HTTP cookies.
7. Угроза избыточного выделения оперативной памяти.
8. Угроза изменения системных и глобальных переменных.
9. Угроза искажения XML-схемы.
10. Угроза искажения вводимой и выводимой на периферийные устройства информации.
11. Угроза использования механизмов авторизации для повышения привилегий.
12. Угроза использования слабостей протоколов сетевого/локального обмена данными.
13. Угроза нарушения изоляции пользовательских данных внутри виртуальной машины.
14. Угроза нарушения процедуры аутентификации субъектов виртуального

информационного взаимодействия.

15. Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин.

16. Угроза нарушения целостности данных кеша.

17. Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов.

18. Угроза некорректного задания структуры данных транзакции.

19. Угроза неправомерных действий в каналах связи.

20. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.

21. Угроза несанкционированного доступа к аутентификационной информации.

22. Угроза несанкционированного доступа к виртуальным каналам передачи.

23. Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети.

24. Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение.

25. Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети.

26. Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин.

27. Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети.

28. Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации.

29. Угроза несанкционированного управления буфером.

30. Угроза несанкционированного управления синхронизацией и состоянием.

31. Угроза несанкционированного управления указателями.

32. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.

33. Угроза обнаружения хостов.

34. Угроза обхода некорректно настроенных механизмов аутентификации.

35. Угроза опосредованного управления группой программ через совместно используемые данные.

36. Угроза определения типов объектов защиты.

37. Угроза определения топологии вычислительной сети.

38. Угроза ошибки обновления гипервизора.

39. Угроза перехвата данных, передаваемых по вычислительной сети.

40. Угроза повреждения системного реестра.

41. Угроза подмены действия пользователя путем обмана.

42. Угроза подмены доверенного пользователя.

43. Угроза подмены субъекта сетевого доступа.

44. Угроза получения предварительной информации об объекте защиты.

45. Угроза приведения системы в состояние «отказ в обслуживании».

46. Угроза пропуска проверки целостности программного обеспечения.

47. Угроза сбоя обработки специальным образом измененных файлов.

48. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов.

49. Угроза утраты вычислительных ресурсов.

50. Угроза заражения компьютера при посещении неблагонадежных сайтов.
51. Угроза неправомерного шифрования информации.
52. Угроза скрытного включения вычислительного устройства в состав бот-сети.
53. Угроза распространения «почтовых червей».
54. Угроза «спама» веб-сервера.
55. Угроза «фарминга».
56. Угроза «фишинга».
57. Угроза несанкционированной модификации защищаемой информации.

Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы безопасности Российской Федерации

Таблица 1. Обобщенные возможности источников атак

№ п/п	Обобщенные возможности источников атак	Да/нет
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы средства криптографической защиты информации (далее - СКЗИ) и среда их функционирования	Да
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	Нет
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

Таблица 2. Актуальные угрозы безопасности персональных данных

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1.	Проведение атаки при нахождении в пределах контролируемой	Актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	зоны		
1.2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования СКЗИ (далее - СФ); помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИи СФ	Не актуально	- Проводятся работы по подбору персонала; - доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; - документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; - помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; - утвержден перечень лиц, имеющих право доступа в помещения
1.3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Не актуально	- Проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается ресурсы информационных систем персональных данных (далее - ИСПДн), обеспечивается в соответствии с контрольнопропускным режимом; - сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; - сотрудники проинформированы об ответствен-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			ности за несоблюдение правил обеспечения безопасности информации
1.4.	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и	Не актуально	- Проводятся работы по подбору персонала; - помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного доступа
2.1.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Не актуально	- Проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода
2.2.	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	- Проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации
3.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Не актуально	- Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			на замок и их открытие только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; - осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей; - на АРМ и серверах, на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты
3.2.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	- Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
3.3.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	Не актуально	- Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности
4.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Не актуально	- Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности; - проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники,

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; - осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей; - на АРМ и серверах, на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты
4.2.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3.	Возможность воздействовать на любые компоненты СКЗИ и СФ	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

Приложение 2 к постановлению
Департамента имущественных и
земельных отношений Курганской области
от 8 августа 2017 года № 42
«Об определении угроз безопасности
персональных данных, актуальных при
обработке персональных данных в
информационных системах персональных
данных, эксплуатируемых при
осуществлении соответствующих видов
деятельности, с учетом содержания
персональных данных, характера и
способов их обработки в Департаменте
имущественных и земельных отношений
Курганской области и подведомственных
Департаменту имущественных и
земельных отношений Курганской области
государственных предприятиях»

Общие положения и актуальные угрозы безопасности персональных данных, определяемые согласно требованиям действующего законодательства

1. Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Департамента имущественных и земельных отношений Курганской области и подведомственных Департаменту имущественных и земельных отношений Курганской области государственных предприятиях (далее — УПДн), разработаны в соответствии с частью 5 статьи 19 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных».

2. УПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) в Департаменте имущественных и земельных отношений Курганской и подведомственных Департаменту имущественных и земельных отношений Курганской области государственных предприятиях (далее — Департамент и подведомственные предприятия).

3. УПДн подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных при их обработке в ИСПДн.

При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно - функциональных характеристик конкретной ИСПДн, применяемых в ней информационных технологий и особенностей её функционирования. По результатам анализа делается вывод об актуальности УПДн для каждой ИСПДн.

В частной модели угроз безопасности персональных данных указываются:

- описание ИСПДн и её структурно-функциональных характеристик;

- описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения

свойств безопасности информации.

4. Актуальные угрозы безопасности персональных данных, обрабатываемые в ИСПДн, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. При уточнении УПДн используется банк данных угроз безопасности информации bdu.fstec.ru.

В Департаменте и подведомственных предприятиях эксплуатируются информационные системы, в которых обрабатываются персональные данные (далее - ПДн).

ИСПДн Департамент и подведомственные предприятия имеют подключения к сетям международного информационного обмена.

Ввод ПДн осуществляется с бумажных и с электронных носителей информации.

Информационный обмен по сетям международного информационного обмена осуществятся с использованием средств криптографической защиты информации (далее - СКЗИ).

Контролируемой зоной ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны находятся автоматизированные рабочие места пользователей, сервера систем, СКЗИ, сетевое и телекоммуникационное оборудование. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и сетям международного информационного обмена.

Категории обрабатываемых ПДн: общедоступные, иные. Актуальны угрозы 3, 4 типа. Уровень защищенности ИСПДн: 4.

Для защиты ПДн в ИСПДн Департамента и подведомственных предприятий используются средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия, проведена оценка эффективности реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн.

5. Актуальные угрозы безопасности ПДн в ИСПДн.

Для ИСПДн Департамента и подведомственных учреждений необходимо обеспечить конфиденциальность, целостность и доступность ПДн.

Под актуальными угрозами безопасности ПДн понимаются совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.

2. Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю Российской Федерации

Суперкомпьютеры, грид-системы, оборудование с числовым программным управлением, беспроводные сети, автоматизированные системы управления технологическими процессами в ИСПДн Департамента и подведомственных предприятиях не используются.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
003	Угроза анализа криптографических алгоритмов и их реализации. Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	не актуально	доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом
004	Угроза аппаратного сброса пароля BIOS. Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера	не актуально	в помещения где обрабатываются персональные данные имеют доступ только доверенные лица
005	Угроза внедрения вредоносного кода в BIOS. Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями	не актуально	ремонт и обслуживание компьютеров осуществляется специалистами организации

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера		
006	Угроза внедрения кода или данных. Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями или автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.), а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов. Данная угроза обусловлена наличием уязвимостей программного обеспечения, а также слабостями мер антивирусной защиты. Реализация данной угрозы возможна в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников, или при наличии у него привилегий установки программного обеспечения	актуально	
007	Угроза воздействия на программы с высокими привилегиями. Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путём использования ошибок в программах и выполнения произвольного кода с их привилегиями. Данная угроза обусловлена слабостями	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	механизма проверки входных данных и команд, а также мер по разграничению доступа. Реализация данной угрозы возможна при условиях: - обладания дискредитируемой программой повышенными привилегиями в системе; - осуществления дискредитируемой программой приёма входных данных от других программ или от пользователя; - нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе		
008	Угроза восстановления аутентификационной информации. Угроза заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: - время подбора в основном определяется не объёмом аутентификационной информации, а объёмом данных её хеш-кода; - восстановленная аутентификационная информация может не совпадать с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную»	актуально	
009	Угроза восстановления предыдущей уязвимой версии BIOS. Угроза заключается в возможности осуще-	не актуально	BIOS защищен паролем; обновление BIOS запрещено;

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ствления вынужденного перехода на использование BIOS/UEFI, содержащей уязвимости. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. При использовании технологии обновления BIOS/UEFI возможно возникновение следующей ситуации (условия, характеризующие ситуацию указаны в хронологическом порядке): - на компьютере установлена некоторая версия BIOS/UEFI, для которой на момент её работы не известны уязвимости; - в силу некоторых обстоятельств BIOS/UEFI проходит процедуру обновления, сохраняя при этом предыдущую версию BIOS/UEFI на случай «отката» системы; - публикуются данные о существовании уязвимостей в предыдущей версии BIOS/UEFI; - происходит сбой в работе системы, в результате чего текущая (новая) версия BIOS/UEFI становится неработоспособной (например, нарушается её целостность); - пользователь осуществляет штатную процедуру восстановления работоспособности системы – проводит «откат» системы к предыдущему работоспособному состоянию		в помещения где обрабатываются персональные данные имеют доступ только доверенные лица
010	Угроза выхода процесса за пределы виртуальной машины. Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора. Данная угроза обусловлена уязвимостями программного обеспечения гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабостями инструкций аппаратной поддержки виртуа-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	лизации на уровне процессора. Реализация данной угрозы приводит не только к компрометации гипервизора, но и запущенных в созданной им виртуальной среде средств защиты, а, следовательно, к их неспособности выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора		
012	Угроза деструктивного изменения конфигурации/среды окружения программ. Угроза заключается в возможности деструктивного программного воздействия на дискредитируемое приложение путём осуществления манипуляций с используемыми им конфигурационными файлами или библиотеками. Данная угроза обусловлена слабостями мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями. Реализация данной угрозы возможна в случае наличия у нарушителя прав осуществления записи в файловые объекты, связанные с конфигурацией/средой окружения программы, или возможности перенаправления запросов дискредитируемой программы от защищённых файловых объектов к ложным	не актуально	у нарушителя отсутствуют права осуществления записи в файловые объекты, связанные с конфигурацией/средой окружения программ
013	Угроза деструктивного использования декларированного функционала BIOS. Угроза заключается в возможности неправомерного использования декларированного функционала BIOS/UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве компьютера. Данная угроза обусловлена уязвимостями программного обеспечения BIOS/UEFI, предназначенного для тестирования и обслуживания компьютера (средств проверки	не актуально	BIOS защищен паролем; обновление BIOS запрещено

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	целостности памяти, программного обеспечения управления RAID-контроллером и т.п.). Реализации данной угрозы может способствовать возможность обновления некоторых BIOS/UEFI без прохождения аутентификации		
014	Угроза длительного удержания вычислительных ресурсов пользователями. Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загруженном состоянии путём осуществления им многократного выполнения определённых деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачами. Данная угроза обусловлена слабостями механизмов балансировки нагрузки и распределения вычислительных ресурсов. Реализация угрозы возможна в случае, если у нарушителя имеется возможность делать запросы, которые в совокупности требуют больше времени на выполнение, чем запросы пользователя	не актуально	реализуются механизмы балансировки нагрузки и распределения вычислительных ресурсов
015	Угроза доступа к защищаемым файлам с использованием обходного пути. Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при условиях:	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	- наличие у нарушителя прав доступа к некоторым объектам файловой системы; - отсутствие проверки вводимых пользователем данных; - наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью		
016	Угроза доступа к локальным файлам сервера при помощи URL. Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделён при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю. Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	не актуально	у нарушителя отсутствуют привилегии на отправку запросов браузеру
017	Угроза доступа/перехвата/изменения HTTP cookies. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя). Данная угроза обусловлена слабостями мер защиты cookies-файлов - отсутствием	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	проверки вводимых данных со стороны сетевой службы, использующей cookies-файлы, а также отсутствием шифрования при передаче cookies-файлов. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к cookies-файлам и отсутствии проверки целостности их значений со стороны дискредитируемого приложения		
018	Угроза загрузки нештатной операционной системы. Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки BIOS/UEFI – указания источника загрузки операционной системы	не актуально	у нарушителя отсутствует возможность выбора источника загрузки операционной системы
019	Угроза заражения DNS-кеша. Угроза заключается в возможности перенаправления нарушителем сетевого трафика через собственный сетевой узел путём опосредованного изменения таблиц соответствия IP- и доменных имён, хранимых в DNS-сервере, за счёт генерации лавины возможных ответов на запрос DNS-сервера легальному пользователю или за счёт эксплуатации уязвимостей DNS-сервера. Данная угроза обусловлена слабостями механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостями DNS-сервера, позволяющими напрямую заменить DNS-кеш DNS-серве-	не актуально	у нарушителя отсутствуют привилегии, достаточные для отправки сетевых запросов к DNS-серверу

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ра. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий, достаточных для отправки сетевых запросов к DNS-серверу		
020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг	не актуально	нарушитель не имеет прав на установку и запуск вредоносного программного обеспечения на облачном сервере
021	Угроза злоупотребления доверием потребителей облачных услуг Угроза заключается в возможности нарушения (случайно или намеренно) защищённости информации потребителей облачных услуг внутренними нарушителями поставщика облачных услуг. Данная угроза обусловлена тем, что значительная часть функций безопасности переведена в сферу ответственности поставщика облачных услуг, а также невозможностью принятия потребителем облачных услуг мер защиты от действий сотрудников	не актуально	поставщик облачных услуг реализует мероприятия по защите информации

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	поставщика облачных услуг. Реализация данной угрозы возможна при условии того, что потребители облачных услуг не входят в состав организации, осуществляющей оказание данных облачных услуг (т.е. потребитель действительно передал поставщику собственную информацию для осуществления её обработки)		
022	Угроза избыточного выделения оперативной памяти. Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей. Данная угроза обусловлена наличием слабостей механизма контроля выделения оперативной памяти различным программам. Реализация данной угрозы возможна при условии нахождения вредоносного программного обеспечения в системе в активном состоянии	актуально	
023	Угроза изменения компонентов системы. Угроза заключается в возможности получения нарушителем доступа к сети Интернет (при его отсутствии в системе), к хранимым на личных мобильных устройствах файлах, внедрения закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы, что в дальнейшем позволит осуществлять данному нарушителю (или другому – внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе. Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной	не актуально	у нарушителя отсутствуют привилегии, достаточные для получения необходимых полномочий

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	конфигурации информационной системы. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий в системе		
024	Угроза изменения режимов работы аппаратных элементов компьютера. Угроза заключается в возможности изменения нарушителем режимов работы аппаратных элементов компьютера путём несанкционированного переконфигурирования BIOS/UEFI, что позволяет: - за счёт изменения частоты системной шины, режима передачи данных по каналам связи и т.п. повлиять на общую производительность компьютера или вызвать сбои в его работе; - за счёт понижения входного напряжения, отключения систем охлаждения временно обеспечить неработоспособность компьютера; за счёт задания недопустимых параметров работы устройств (порогового значения отключения устройства при перегреве, входного напряжения и т.п.) привести к физическому выходу из строя отдельных аппаратных элементов компьютера. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение соответствующих параметров настройки BIOS/UEFI	не актуально	BIOS защищен паролем; в помещения где обрабатываются персональные данные имеют доступ только доверенные лица
025	Угроза изменения системных и глобальных переменных. Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных.	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Данная угроза обусловлена слабостями механизма контроля доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к системным и глобальным переменным и отсутствии проверки целостности их значений со стороны дискредитируемого приложения		
026	Угроза искажения XML-схемы. Угроза заключается в возможности изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером. Данная угроза обусловлена слабостями мер обеспечения целостности передаваемых при клиент-серверном взаимодействии данных, а также слабостями механизма сетевого взаимодействия открытых систем. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к сетевому трафику, передаваемому между клиентом и сервером и отсутствии проверки целостности XML-схемы со стороны дискредитируемого приложения	актуально	
027	Угроза искажения вводимой и выводимой на периферийные устройства информации. Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, по-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок		
028	Угроза использования альтернативных путей доступа к ресурсам. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных. Реализация данной угрозы возможна при условии наличия у нарушителя: - возможности ввода произвольных данных в адресную строку; - сведений о пути к защищаемому ресурсу; возможности изменения интерфейса ввода входных данных	не актуально	нарушитель не обладает возможностями ввода произвольных данных в адресную строку, изменения интерфейса ввода входных данных, сведениями о пути к защищаемому ресурсу
030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию. Угроза заключается в возможности прохо-	не актуально	устройства с идентификационной и аутентификационной информацией «по умол-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ждения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: - наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты; - успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты		чанию» отсутствуют; пользователи не имеют доступа к сетевым устройствам
031	Угроза использования механизмов авторизации для повышения привилегий. Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки.	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе		
032	Угроза использования поддельных цифровых подписей BIOS. Угроза заключается в возможности установки уязвимой версии обновления BIOS/UEFI или версии, содержащей вредоносное программное обеспечение, но имеющей цифровую подпись. Данная угроза обусловлена слабостями мер по контролю за благонадёжностью центров выдачи цифровых подписей. Реализация данной угрозы возможна при условии выдачи неблагонадёжным центром сертификации цифровой подписи на версию обновления BIOS/UEFI, содержащую уязвимости, или на версию, содержащую вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений	не актуально	обновление BIOS запрещено
033	Угроза использования слабостей кодирования входных данных. Угроза заключается в возможности осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.). Данная угроза обусловлена слабостями механизма контроля входных данных. Реализация данной угрозы возможна при условиях: - дискредитируемая система принимает входные данные от нарушителя; - нарушитель обладает возможностью	не актуально	реализуется контроль входных данных

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	управления одним или несколькими параметрами входных данных		
034	Угроза использования слабостей протоколов сетевого/локального обмена данными. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Данная угроза обусловлена слабостями самих протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов, или уязвимостями, внедряемыми автоматизированными средствами проектирования / разработки. Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными	актуально	
035	Угроза использования слабых криптографических алгоритмов BIOS. Угроза заключается в сложности проверки реальных параметров работы и алгоритмов, реализованных в криптографических средствах BIOS/UEFI. При этом доверие к криптографической защите будет ограничено доверием к производителю BIOS. Данная угроза обусловлена сложностью использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI. Возможность реализации данной угрозы снижает достоверность оценки реального уровня защищённости системы	не актуально	BIOS защищен паролем; в помещения где обрабатываются персональные данные имеют доступ только доверенные лица
036	Угроза исследования механизмов работы программы. Угроза заключается в возможности проведения нарушителем обратного инжиниринга кода программы и дальнейшего иссле-	не актуально	у нарушителя отсутствует доступа к исходным файлам программ, дистрибутивам программ

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	дования его структуры, функционала и состава в интересах определения алгоритма работы программы и поиска в ней уязвимостей. Данная угроза обусловлена слабостями механизма защиты кода программы от исследования. Реализация данной угрозы возможна в случаях: - наличия у нарушителя доступа к исходным файлам программы; - наличия у нарушителя доступа к дистрибутиву программы и отсутствия механизма защиты кода программы от исследования		
037	Угроза исследования приложения через отчёты об ошибках. Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его предполагаемой структуры путём анализа генерируемых этим приложением отчётов об ошибках. Данная угроза обусловлена размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчётах об ошибках. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	не актуально	у нарушителя отсутствует доступ к отчётам об ошибках, генерируемых приложением
039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS. Угроза заключается в возможности нарушения (невозможности осуществления) процедуры обновления BIOS/UEFI при исчерпании запаса необходимых для её проведения ключей. Данная угроза обусловлена ограниченностью набора ключей, необходимых для обновления BIOS/UEFI.	не актуально	обновление BIOS запрещено

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Реализация данной угрозы возможна путём эксплуатации уязвимостей средств обновления набора ключей, или путём использования нарушителем программных средств перебора ключей		
041	Угроза межсайтового скриптинга. Угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы таким образом, что он будет выполнен на рабочей станции просматривающего этот сайт пользователя. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему	не актуально	выполнение сценариев отключено
042	Угроза межсайтовой подделки запроса. Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя. Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя. Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера	не актуально	аутентификационная информацию не сохраняется в браузере
043	Угроза нарушения доступности облачного сервера	не актуально	поставщик облачных услуг реализует мероприятия

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Угроза заключается в возможности прекращения оказания облачных услуг всем потребителям (или группе потребителей) из-за нарушения доступности для них облачной инфраструктуры. Данная угроза обусловлена тем, что обеспечение доступности не является специфичным требованием безопасности информации для облачных технологий, и, кроме того, облачные системы реализованы в соответствии с сервис-ориентированным подходом. Реализация данной угрозы возможна при переходе одного или нескольких облачных серверов в состояние «отказ в обслуживании». Более того, способность динамически изменять объём предоставляемых потребителям облачных услуг может быть использована нарушителем для реализации угрозы. При этом успешно реализованная угроза в отношении всего лишь одного облачного сервиса позволит нарушить доступность всей облачной системы		по защите информации
044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины. Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины. Данная угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ вирту-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	альной машины не только за счёт эксплуатации уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы		
045	Угроза нарушения изоляции среды исполнения BIOS. Угроза заключается в возможности изменения параметров и (или) логики работы программного обеспечения BIOS/UEFI путём программного воздействия из операционной системы компьютера или путём несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора. Данная угроза обусловлена слабостями технологий разграничения доступа к BIOS/UEFI, его функциям администрирования и обновления, со стороны операционной системы или каналов связи. Реализация данной угрозы возможна: - со стороны операционной системы – при условии наличия BIOS/UEFI функционала обновления и (или) управления программным обеспечением BIOS/UEFI из операционной системы; - со стороны сети – при условии наличия у дискредитируемого серверного сервис-процессора достаточных привилегий для управления всей системой, включая модификацию BIOS/UEFI серверов системы, и дискредитируемого сервера	не актуально	BIOS защищен паролем; обновление BIOS запрещено
046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия. Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия. Данная угроза обусловлена наличием мно-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	жества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между её уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия		
048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин. Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин. Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации. Реализация данной угрозы может привести: - к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов; - к нарушению целостности программ, установленных на виртуальных машинах; - к нарушению доступности ресурсов виртуальных машин; - к созданию ботнета путём внедрения вредоносного программного обеспечения в образы виртуальных машин, используемые в качестве шаблонов (эталонные образы)	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
049	Угроза нарушения целостности данных кеша. Угроза заключается в возможности размещения нарушителем в кеше приложения (например, браузера) или службы (например, DNS или ARP) некорректных (потенциально опасных) данных таким образом, что до обновления кеша дискредитируемое приложение (или служба) будет считать эти данные корректными. Данная угроза обусловлена слабостями в механизме контроля целостности данных в кеше. Реализация данной угрозы возможна в условиях осуществления нарушителем успешного несанкционированного доступа к данным кеша и отсутствии проверки целостности данных в кеше со стороны дискредитируемого приложения (или службы)	актуально	
051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания. Угроза заключается в возможности потери несохранённых данных, обрабатываемых в предыдущей сессии работы на компьютере, а также в возможности потери времени для возобновления работы на компьютере. Данная угроза обусловлена ошибками в реализации программно-аппаратных компонентов компьютера, связанных с обеспечением питания. Реализация данной угрозы возможна при условии невозможности выведения компьютера из промежуточных состояний питания («ждущего режима работы», «гибернации» и др.)	не актуально	промежуточные состояния питания не используются
052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения.	не актуально	нет необходимости в смене поставщика облачных услуг в ближайшей перспек-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Угроза заключается в возможности возникновения у потребителя облачных услуг непреодолимых сложностей для смены поставщика облачных услуг из-за технических сложностей в реализации процедуры миграции образов виртуальных машин из облачной системы одного поставщика облачных услуг в систему другого. Данная угроза обусловлена тем, что каждый поставщик облачных услуг использует для реализации своей деятельности аппаратное и программное обеспечение различных производителей, часть которого может использовать специфические (для данного производителя) инструкции, протоколы, методы, схемы коммутации и другие особенности реализации своего функционала. Реализация данной угрозы возможна в случае несовместимости стандартных программных интерфейсов обмена данными (API) для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях. Также данная угроза обуславливает ограничение возможности смены производителей аппаратного и программного обеспечения поставщиком облачных услуг, что может привести к нарушению целостности и доступности информации по вине поставщика облачных услуг		тиве
053	Угроза невозможности управления правами пользователей BIOS. Угроза заключается в возможности неправомерного использования пользователями декларированного функционала BIOS/UEFI, ориентированного на администраторов. Данная угроза обусловлена слабостями технологий разграничения доступа (распределения прав) к функционалу BIOS/UEFI между различными пользователями и администраторами.	не актуально	BIOS защищен паролем; в помещения где обрабатываются персональные данные имеют доступ только доверенные лица

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Реализация данной угрозы возможна при условии физического доступа к терминалу и, при необходимости, к системному блоку компьютера		
054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг Угроза заключается в возможности раскрытия или повреждения целостности поставщиком облачных услуг защищаемой информации потребителей облачных услуг, невыполнения требований к уровню качества (уровню доступности) предоставляемых потребителям облачных услуг доступа к их программам или иммигрированным в облако информационным системам. Данная угроза обусловлена невозможностью непосредственного контроля над действиями сотрудников поставщика облачных услуг со стороны их потребителей. Реализация данной угрозы возможна в случаях халатности со стороны сотрудников поставщика облачных услуг, недостаточности должностных и иных инструкций данных сотрудников, недостаточности мер по менеджменту и обеспечению безопасности облачных услуг и т.д.	не актуально	поставщик облачных услуг реализует мероприятия по защите информации
055	Угроза незащищённого администрирования облачных услуг Угроза заключается в возможности осуществления опосредованного деструктивного программного воздействия на часть или все информационные системы, функционирующие в облачной среде, путём перехвата управления над облачной инфраструктурой через механизмы удалённого администрирования. Данная угроза обусловлена недостаточностью внимания, уделяемого контролю вводимых пользователями облачных услуг данных (в том числе аутентификационных данных), а также уязвимостями небезопас-	не актуально	поставщик облачных услуг реализует мероприятия по защите информации

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ных интерфейсов обмена данными (API), используемых средствами удалённого администрирования. Реализация данной угрозы возможна в случае получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования		
056	Угроза некачественного переноса инфраструктуры в облако. Угроза заключается в возможности снижения реального уровня защищённости иммигрирующей в облако информационной системы из-за ошибок, допущенных при миграции в ходе преобразования её реальной инфраструктуры в облачную. Данная угроза обусловлена тем, что преобразование даже части инфраструктуры информационной системы в облачную зачастую требует проведения серьёзных изменений в такой инфраструктуре (например, в политиках безопасности и организации сетевого обмена данными). Реализация данной угрозы возможна в случае несовместимости программных и сетевых интерфейсов или несоответствий политик безопасности при осуществлении переноса информационной системы в облако	не актуально	нет необходимости в смене поставщика облачных услуг в ближайшей перспективе
058	Угроза неконтролируемого роста числа виртуальных машин. Угроза заключается в возможности ограничения или нарушения доступности виртуальных ресурсов для конечных потребителей облачных услуг путём случайного или несанкционированного преднамеренного создания нарушителем множества виртуальных машин. Данная угроза обусловлена ограниченностью объёма дискового пространства, выделенного под виртуальную инфраструкту-	не актуально	у нарушителя отсутствуют права на создание виртуальных машин в облачной инфраструктуре

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ру, и слабостями технологий контроля процесса создания виртуальных машин. Реализация данной угрозы возможна при условии наличия у нарушителя прав на создание виртуальных машин в облачной инфраструктуре		
059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов. Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). Данная угроза обусловлена уязвимостями программного обеспечения уровня управления виртуальной инфраструктурой, реализующего функцию распределения компьютерных ресурсов между пользователями. Реализация данной угрозы возможна при условии успешного осуществления нарушителем несанкционированного доступа к программному обеспечению уровня управления виртуальной инфраструктурой, реализующему функцию распределения компьютерных ресурсов между пользователями	актуально	
061	Угроза некорректного задания структуры данных транзакции. Угроза заключается в возможности совершения нарушителем (клиентом базы данных) подлога путём прерывания транзакции или подмены идентификатора транзакции. В первом случае происходит неполное выполнение транзакции, а во втором – пользователь форсированно завершает транзакцию, изменяя её ID, и сообщая о том, что транзакция не была проведена, тем самым провоцируя повторное	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	проведение транзакции. Данная угроза обусловлена слабостями механизма контроля непрерывности транзакций и целостности данных, передаваемых в ходе транзакции между базой данных и её клиентом		
062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера. Угроза заключается в возможности перенаправления или копирования обрабатываемых браузером данных через прозрачный прокси-сервер, подключённый к браузеру в качестве плагина. Данная угроза обусловлена слабостями механизма контроля доступа к настройкам браузера. Реализация возможна в случае успешного осуществления нарушителем включения режима использования прозрачного прокси-сервера в параметрах настройки браузера, например, в результате реализации угрозы межсайтового скриптинга	не актуально	выполнение сценариев отключено
063	Угроза некорректного использования функционала программного обеспечения. Угроза заключается в возможности использования декларированных возможностей программных и аппаратных средств определённым (нестандартным, некорректным) способом с целью деструктивного воздействия на информационную систему и обрабатываемую ею информацию. Данная угроза связана со слабостями механизма обработки данных и команд, вводимых пользователями. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к программным и аппаратным средствам	не актуально	механизм обработки данных и команд, вводимых пользователями защищен от некорректного использования
064	Угроза некорректной реализации политики лицензирования в облаке. Угроза заключается в возможности отказа	не актуально	потребитель облачных услуг не имеет прав на установку про-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	потребителям облачных услуг в удалённом доступе к арендуемому программному обеспечению (т.е. происходит потеря доступности облачной услуги SaaS) по вине поставщика облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками лицензирования использования программного обеспечения различных производителей в облаке. Реализация данной угрозы возможна при условии, что политика лицензирования использования программного обеспечения основана на ограничении количества его установок или числа его пользователей, а созданные виртуальные машины с лицензируемым программным обеспечением использованы много раз		граммного обеспечения в облаке
065	Угроза неопределённости в распределении ответственности между ролями в облаке. Угроза заключается в возможности возникновения существенных разногласий между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей в части обеспечения информационной безопасности. Данная угроза обусловлена отсутствием достаточного набора мер контроля за распределением ответственности между различными ролями в части владения данными, контроля доступа, поддержки облачной инфраструктуры и т. п. Возможность реализации данной угрозы повышается в случае использования облачных услуг, предоставляемых другими поставщиками (т.е. в случае использования схемы оказания облачных услуг с участием посредников)	не актуально	поставщик облачных услуг реализует мероприятия по защите информации
066	Угроза неопределённости ответственности за обеспечение безопасности облака. Угроза заключается в возможности невы-	не актуально	поставщик облачных услуг реализует мероприятия по защите инфор-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	полнения ряда мер по защите информации как поставщиком облачных услуг, так и их потребителем. Данная угроза обусловлена отсутствием чёткого разделения ответственности в части обеспечения безопасности информации между потребителем и поставщиком облачных услуг. Реализация данной угрозы возможна при условии недостаточности документального разделения сфер ответственности между сторонами участвующими в оказании облачных услуг, а также отсутствия документального определения ответственности за несоблюдение требований безопасности		мации
067	Угроза неправомерного ознакомления с защищаемой информацией. Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.	не актуально	приняты организационные меры по затруднению просмотра экранов мониторов посторонними лицам
068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением. Угроза заключается в возможности осуще-	не актуально	нарушитель не имеет доступа к API

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ствления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). Данная угроза обусловлена наличием слабостей в механизме проверки входных данных и команд API, используемого программным обеспечением. Реализация данной угрозы возможна в условиях наличия у нарушителя доступа к API и отсутствия у дискредитируемого приложения механизма проверки вводимых данных и команд		
069	Угроза неправомерных действий в каналах связи. Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	актуально	
070	Угроза непрерывной модернизации облачной инфраструктуры Угроза заключается в возможности занесения в облачную систему уязвимостей и слабостей вместе с добавлением нового программного или аппаратного обеспечения. При этом система, рассматриваемая как защищённая на этапе ввода её в эксплуатацию, уже не может считаться тако-	не актуально	поставщик облачных услуг реализует мероприятия по защите информации

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	вой после её модернизации. Данная угроза обусловлена тем, что, во-первых, поставщики облачных услуг предоставляют возможность осуществления потребителем облачных услуг выбора и (или) изменения первоначального состава программного обеспечения облачной инфраструктуры в процессе оказания таких услуг, а, во-вторых, при интенсивном подключении новых потребителей модернизация облачной инфраструктуры может проходить несколько раз в год. Реализация данной угрозы возможна в случае, если срок до следующей модернизации не превышает срока проведения оценки соответствия системы требованиям безопасности в условиях отсутствия системы менеджмента облачных услуг и обеспечения их безопасности (системы облачного менеджмента)		
071	Угроза несанкционированного восстановления удалённой защищаемой информации. Угроза заключается в возможности осуществления прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации. Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удалённая с машинного носителя, в большинстве случаев может быть восстановлена. Реализация данной угрозы возможна при следующих условиях: - удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных (например, физическое уничтожение машинного носителя информации);	не актуально	удаление информации с машинного носителя происходило с использованием способов (методов, алгоритмов) гарантированного стирания данных

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	- технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; - информация не хранилась в криптографически преобразованном виде		
072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS. Угроза заключается в возможности внедрения в BIOS/UEFI вредоносного программного кода после ошибочного или злонамеренного выключения пользователем механизма защиты BIOS/UEFI от записи, а также в возможности установки неподписанного обновления в обход механизма защиты от записи в BIOS/UEFI. Данная угроза обусловлена слабостями мер по разграничению доступа к управлению механизмом защиты BIOS/UEFI от записи, а также уязвимостями механизма обновления BIOS/UEFI, приводящими к переполнению буфера. Реализация данной угрозы возможна в одном из следующих условий: - выключенном механизме защиты BIOS/UEFI от записи; - успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера	не актуально	BIOS защищен паролем; обновление BIOS запрещено; в помещения где обрабатываются персональные данные имеют доступ только доверенные лица
073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети. Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём эксплуатации уязви-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	мостей программного и (или) микропрограммного обеспечения указанного оборудования. Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования		
074	Угроза несанкционированного доступа к аутентификационной информации. Угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации. Данная угроза обусловлена наличием слабостей мер разграничения доступа к защищаемой информации. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа к участкам оперативного или постоянного запоминающих устройств, в которых хранится информация аутентификации	актуально	
075	Угроза несанкционированного доступа к виртуальным каналам передачи. Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий. Данная угроза обусловлена слабостями	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации		
076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети. Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети. Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данной угрозы возможна в одном из следующих случаев: - наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин; - наличие у гипервизора активного интерфейса взаимодействия с физической вы-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	числительной сетью		
077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение. Угроза заключается в возможности нарушения вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) других виртуальных машин, функционирующих под управлением того же гипервизора, а также изменения параметров её (их) настройки. Данная угроза обусловлена наличием слабостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной виртуальной машины	актуально	
078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети. Угроза заключается в возможности осуществления нарушителем деструктивного	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия		
079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин. Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе. Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для реализации механизма обмена данными между виртуальными машинами, реализованные в гипервизоре и активированные в системе	актуально	
080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети.	не актуально	у нарушителя отсутствуют привилегии достаточные для осуще-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для осуществления обмена данными в системе, построенной с использованием технологий виртуализации. Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации		ствления обмена данными в системе, построенной с использованием технологий виртуализации
084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети. Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных). Данная угроза обусловлена наличием слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и (или) виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны с высокой сложностью алгоритмов обеспечения согласованности дей-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ствий по распределению информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства. Реализация данной угрозы возможна при условии наличия у нарушителя специальных программных средств, способных эксплуатировать слабостей технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации и др.)		
085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации. Угроза заключается в возможности нарушения конфиденциальности информации, содержащейся в распределённых файлах, содержащих защищаемую информацию, путём восстановления данных распределённых файлов из их множества отдельных фрагментов с помощью программного обеспечения и информационных технологий по обработке распределённой информации. Данная угроза обусловлена тем, что в связи с применением множества технологий виртуализации, предназначенных для работы с данными (распределение данных внутри виртуальных и логических дисков, распределение данных между такими дисками, распределение данных между физическими и виртуальными накопителями единого дискового пространства, выделение областей дискового пространства в виде отдельных дисков и др.), практически все файлы хранятся в виде множества отдельных сегментов. Реализация данной угрозы возможна при условии недостаточности или отсутствия мер по обеспечению конфиденциальности информации, хранящейся на отдельных	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	накопителях		
086	Угроза несанкционированного изменения аутентификационной информации. Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учётной записью дискредитированного пользователя	не актуально	пользователи не имеют прав на установку программного обеспечения
087	Угроза несанкционированного использования привилегированных функций BIOS. Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI. Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала	не актуально	BIOS защищен паролем; в помещения где обрабатываются персональные данные имеют доступ только доверенные лица
088	Угроза несанкционированного копирования защищаемой информации. Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер	не актуально	в помещения где обрабатываются персональные данные имеют доступ только доверенные лица

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде		
089	Угроза несанкционированного редактирования реестра. Угроза заключается в возможности внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом. При этом под реестром понимается не только реестр операционной системы Microsoft Windows, а любой реестр, используемый приложением. Изменение реестра может быть как этапом при осуществлении другого деструктивного воздействия, так и основной целью. Данная угроза обусловлена слабостями механизма контроля доступа, заключающимися в присвоении реализующим его программам слишком высоких привилегий при работе с реестром. Реализация данной угрозы возможна в случае получения нарушителем прав на работу с программой редактирования реестра	не актуально	пользователи не обладают привилегиями по доступу к реестрам
090	Угроза несанкционированного создания учётной записи пользователя. Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации.	не актуально	у пользователей отсутствуют права на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)		
091	Угроза несанкционированного удаления защищаемой информации. Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путём осуществления деструктивного программного или физического воздействия на машинный носитель информации. Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	не актуально	доступ к защищаемой информации имеют только доверенные лица
092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам. Угроза заключается в возможности получения нарушителем привилегий управления системой путём использования удалённого внеполосного (по независимому вспомогательному каналу TCP/IP) доступа. Данная угроза обусловлена невозможностью контроля за механизмом, реализующего функции удалённого доступа на	не актуально	технологию удалённого внеполосного доступа не используется

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	аппаратном уровне, на уровне операционной системы, а также независимостью от состояния питания аппаратных устройств, т.к. данный механизм предусматривает процедуру удалённого включения/выключения аппаратных устройств. Реализация данной угрозы возможна в условиях: - наличия в системе аппаратного обеспечения, поддерживающего технологию удалённого внеполосного доступа; - наличия подключения системы к сетям общего пользования (сети Интернет)		
093	Угроза несанкционированного управления буфером. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного воздействия на систему (например, переполнение буфера для выполнения произвольного вредоносного кода). Данная угроза обусловлена слабостями в механизме разграничения доступа к буферу обмена, а также слабостями в механизмах проверки вводимых данных. Реализация данной угрозы возможна в случае осуществления нарушителем успешного несанкционированного доступа к сегменту оперативной памяти дискредитируемого объекта, в котором расположен буфер обмена	актуально	
094	Угроза несанкционированного управления синхронизацией и состоянием. Угроза заключается в возможности изменения нарушителей последовательности действий, выполняемых дискредитируемыми приложениями, использующими в своей работе технологии управления процессами на основе текущего времени и состо-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	яния информационной системы (например, текущих значений глобальных переменных, наличия запущенных процессов и др.). Данная угроза основана на слабостях механизма управления синхронизацией и состоянием, позволяющих нарушителю вносить изменения в его работу в определённые промежутки времени. Реализация данной угрозы возможна при условии наличия у нарушителя возможности: - контролировать состояние дискредитируемого приложения (этапы выполнения алгоритма); - отслеживать моменты времени, когда дискредитируемое приложение временно прерывает свою работу с глобальными данными; выполнить деструктивные действия в определённые моменты времени (например, внести изменения в файл с данными или изменить содержимое ячейки памяти)		
095	Угроза несанкционированного управления указателями. Угроза заключается в возможности выполнения нарушителем произвольного вредоносного кода от имени дискредитируемого приложения или приведения дискредитируемого приложения в состояние «отказ в обслуживании» путём изменения указателей на ячейки памяти, содержащие определённые данные, используемые дискредитируемым приложением. Данная угроза связана с уязвимостями в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение указателей, используемых дискредитируемым приложением	актуально	
096	Угроза несогласованности политик без-	не актуально	поставщик облач-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	опасности элементов облачной инфраструктуры Угроза заключается в возможности осуществления нарушителем деструктивных программных воздействий как в отношении поставщиков, так и потребителей облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками безопасности элементов облачной инфраструктуры вследствие значительной распределённости облачной инфраструктуры. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)		ных услуг реализует мероприятия по защите информации
098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб. Угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика		
099	Угроза обнаружения хостов. Угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика	актуально	
100	Угроза обхода некорректно настроенных механизмов аутентификации. Угроза заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). Данная угроза обусловлена в случае некорректных значений параметров конфигурации средств аутентификации и/или отсутствием контроля входных данных. Реализация данной угрозы возможна при условии наличия ошибок в заданных значениях параметров настройки механизмов	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	аутентификации		
101	Угроза общедоступности облачной инфраструктуры Угроза заключается в возможности осуществления несанкционированного доступа к защищаемой информации одного потребителя облачных услуг со стороны другого. Данная угроза обусловлена тем, что из-за особенностей облачных технологий потребителям облачных услуг приходится совместно использовать одну и ту же облачную инфраструктуру. Реализация данной угрозы возможна в случае допущения ошибок при разделении элементов облачной инфраструктуры между потребителями облачных услуг, а также при изоляции их ресурсов и обособлении данных друг от друга	не актуально	поставщик облачных услуг реализует мероприятия по защите информации
102	Угроза опосредованного управления группой программ через совместно используемые данные. Угроза заключается в возможности опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные, файлы конфигурации и др.). Данная угроза обусловлена наличием слабостей в механизме контроля внесённых изменений в общие данные каждой из программ в группе. Реализация данной угрозы возможна в случае успешного перехвата нарушителем управления над одной из программ в группе программ, использующих общие данные	актуально	
103	Угроза определения типов объектов защиты. Угроза заключается в возможности проведения нарушителем анализа выходных	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	данных дискредитируемой системы с помощью метода, позволяющего определить точные значения параметров и свойств, однозначно присущих дискредитируемой системе (данный метод известен как «fingerprinting», с англ. «дактилоскопия»). Использование данного метода не наносит прямого вреда дискредитируемой системе. Однако сведения, собранные таким образом, позволяют нарушителю выявить слабые места дискредитируемой системы, которые могут быть использованы в дальнейшем при реализации других угроз.Данная угроза обусловлена ошибками в параметрах конфигурации средств межсетевого экранирования, а также с отсутствием механизмов контроля входных и выходных данных. Реализация данной угрозы возможна в случае наличия у нарушителя сведений о взаимосвязи выходных данных с конфигурацией дискредитируемой системы (документация на программные средства, стандарты передачи данных, спецификации и т.п.)		
104	Угроза определения топологии вычислительной сети. Угроза заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями средств межсетевого экранирования (алгоритма работы и конфигурации правил фильтрации сетевого трафика). Реализация данной угрозы возможна в	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	случае наличия у нарушителя возможности подключения к исследуемой вычислительной сети и наличием специализированного программного обеспечения, реализующего функцию анализа сетевого трафика		
108	Угроза ошибки обновления гипервизора. Угроза заключается в возможности дискредитации нарушителем функционирующих на базе гипервизора защитных механизмов, предотвращающих несанкционированный доступ к образам виртуальных машин, из-за ошибок его обновления. Данная угроза обусловлена зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или её части, если используется более одного гипервизора) от работоспособности гипервизора. Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: - сбоев в процессе его обновления; - обновлений, в ходе которых внедряются новые ошибки в код гипервизора; - обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования; - других инцидентов безопасности информации	актуально	
109	Угроза перебора всех настроек и параметров приложения. Угроза заключается в возможности получения нарушителем доступа к дополнительному скрытому функционалу (информация о котором не была опубликована разработчиком) или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких	не актуально	у нарушителя отсутствуют привилегии на изменение конфигурации программного обеспечения

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	значений параметров путём перебора всех возможных комбинаций. Данная угроза обусловлена уязвимостями программного обеспечения, проявляющимися при его неправильной конфигурации. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение конфигурации программного обеспечения. При реализации данной угрозы, в отличии от других подобных угроз, нарушитель действует «вслепую» – простым путём перебора всевозможных комбинаций		
111	Угроза передачи данных по скрытым каналам. Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы путём её нестандартного (незаметного, скрытого) размещения в легитимно передаваемых по сети (или сохраняемых на отчуждаемые носители) открытых данных путём её маскирования под служебные протоколы, сокрытия в потоке других данных (стеганография) и т. п. Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация данной угрозы возможна при условии наличия у нарушителя прав в дискредитируемой системе: - установки специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации; - доступа к каналам передачи данных	не актуально	у нарушителя отсутствуют привилегии на установку программного обеспечения
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники. Угроза заключается в возможности сброса пользователем (нарушителем) состояния	не актуально	у нарушителя отсутствуют привилегии на осуществление перезагрузки; доступ в помеще-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом. Данная угроза обусловлена свойством оперативной памяти обнулять своё состояние при выключении и перезагрузке. Реализация данной угрозы возможна как аппаратным способом (нажатием кнопки), так и программным (локально или удалённо) при выполнении следующих условий: - наличие в системе открытых сессий работы пользователей; - наличие у нарушителя прав в системе (или физической возможности) на осуществление форсированной перезагрузки		ния где обрабатываются персональные данные имеют только доверенные лица
114	Угроза переполнения целочисленных переменных. Угроза заключается в возможности приведения нарушителем дискредитируемого приложения к сбоям в работе путём подачи на его входные интерфейсы данных неподдерживаемого формата или выполнения с его помощью операции, в результате которой будут получены данные неподдерживаемого дискредитируемым приложением формата. Данная угроза обусловлена уязвимостями программного обеспечения, связанными с недостаточной проверкой такими приложениями корректности входных данных, а также тем, что операторы любого программного обеспечения способны правильно обрабатывать только определённые типы данных (например, только целые или только положительные числа). Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных; - возможности взаимодействия с входным интерфейсом дискредитируемого прило-	не актуально	нарушитель не располагает сведениями о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	жения		
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств. Данная угроза обусловлена недостаточностью мер защиты информации от утечки и контроля потоков данных, а также невозможностью осуществления защиты вводимой и выводимой на периферийные устройства информации с помощью криптографических средств (т.к. представление пользователям системы информации должно осуществляться в доступном для понимания виде). Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.	не актуально	у нарушителя отсутствуют привилегии на установку программного обеспечения
116	Угроза перехвата данных, передаваемых по вычислительной сети. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме (т.е. «прослушивать сетевой трафик») для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых дан-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения. Реализация данной угрозы возможна в следующих условиях: - наличие у нарушителя доступа к дискредитируемой вычислительную сети; - неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных		
117	Угроза перехвата привилегированного потока. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к потоку данных, созданного приложением с дополнительными привилегиями (к привилегированному потоку данных), путём синхронного (вызов привилегированной функции, возвращающей неправильное значение) или асинхронного (создание обратных вызовов, манипулирование указателями и т.п.) деструктивного программного воздействия на него. Данная угроза обусловлена уязвимостями программного обеспечения, использующего в своей работе участки кода, исполняемого с дополнительными правами, наследуемыми создаваемыми привилегированными потоками (наличие ошибочных указателей, некорректное освобождение памяти и т.п.). Реализация данной угрозы возможна в следующих условиях: - в дискредитируемом приложении существуют участки кода, требующие исполне-	не актуально	программное обеспечение получено из доверенных источников

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ния с правами, превышающими права обычных пользователей; - нарушитель обладает привилегиями, позволяющими вносить изменения во входные данные дискредитируемого приложения		
118	Угроза перехвата привилегированного процесса. Угроза заключается в возможности получения нарушителем права управления процессом, обладающим высокими привилегиями (например, унаследованными от пользователя или группы пользователей, выполняющих роль администраторов дискредитируемой системы), для выполнения произвольного вредоносного кода с правами дискредитированного процесса. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации), приводящими к некорректному распределению прав доступа внутри древа наследуемых процессов. Реализация данной угрозы возможна при выполнении одного из условий: - успешного введения нарушителем некорректных данных, приводящих к переполнению буфера или к реализации некоторых типов программных инъекций; - наличия у нарушителя привилегий на запуск системных утилит, предназначенных для управления процессами	не актуально	у нарушителя отсутствуют привилегии на запуск системных утилит
119	Угроза перехвата управления гипервизором. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым гипервизором, за счёт получения нарушителем права управления гипервизором путём	не актуально	у нарушителя отсутствуют права на осуществление взаимодействия с консолью управления гипервизором

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	эксплуатации уязвимостей консоли управления гипервизором. Данная угроза обусловлена наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью управления гипервизором		
120	Угроза перехвата управления средой виртуализации. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым всеми гипервизорами, реализующими среду виртуализации, за счёт получения нарушителем права управления этими гипервизорами путём эксплуатации уязвимостей консоли средства управления виртуальной инфраструктурой. Данная угроза обусловлена наличием у консоли средства управления виртуальной инфраструктурой, реализуемого в рамках одной из виртуальных машин, программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня управления виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью средства управления виртуальной ин-	не актуально	у нарушителя отсутствуют права на осуществление взаимодействия с консолью средства управления виртуальной инфраструктурой

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	фраструктурой		
121	Угроза повреждения системного реестра. Угроза заключается в возможности нарушения доступности части функционала или всей информационной системы из-за повреждения используемого в её работе реестра вследствие некорректного завершения работы операционной системы (неконтролируемая перезагрузка, возникновения ошибок в работе драйверов устройств и т.п.), нарушения целостности файлов, содержащих в себе данные реестра, возникновения ошибок файловой системы носителя информации или вследствие осуществления нарушителем деструктивного программного воздействия на файловые объекты, содержащие реестр. Данная угроза обусловлена слабостями мер контроля доступа к файлам, содержащим данные реестра, мер резервирования и контроля целостности таких файлов, а также мер восстановления работоспособности реестра из-за сбоев в работе операционной системы. Реализация данной угрозы возможна при одном из условий: - возникновения ошибок в работе отдельных процессов или всей операционной системы; - наличии у нарушителя прав доступа к реестру или файлам, содержащим в себе данные реестра	актуально	
122	Угроза повышения привилегий. Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) от его (её) имени путём эксплуатации неправомерно полученных нарушителем дополнительных прав на управление дискредитированным объектом.	не актуально	программное обеспечение получено из доверенных источников

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации). Реализация данной угрозы возможна при наличии у нарушителя программного обеспечения (типа «эксплойт»), специально разработанного для реализации данной угрозы в дискредитируемой системе		
123	Угроза подбора пароля BIOS. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI путём входа в консоль BIOS/UEFI по паролю, подобранному программно или «вручную» с помощью методов тотального перебора вариантов или подбора по словарю. Данная угроза обусловлена слабостями механизма аутентификации, реализуемого в консолях BIOS/UEFI. Реализация данной угрозы возможна в одном из следующих случаев: - нарушитель может осуществить физический доступ к компьютеру и имеет возможность его перезагрузить; - нарушитель обладает специальным программным средством перебора паролей BIOS/UEFI и привилегиями в системе на установку и запуск таких средств	не актуально	в помещения где обрабатываются персональные данные имеют доступ только доверенные лица
124	Угроза подделки записей журнала регистрации событий. Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях) для введения в заблуждение её администраторов или сокрытия следов реализации других угроз. Данная угроза обусловлена недостаточностью мер по разграничению доступа к жур-	не актуально	технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, нарушитель не обладает необходимыми для осуществления записи в файлы журналов привилегиями

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	налу регистрации событий безопасности. Реализация данной угрозы возможна в одном из следующих случаев: - технология ведения журналов регистрации событий безопасности предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями; - технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, но нарушитель обладает привилегиями, необходимыми для осуществления записи в файлы журналов, а также специальными программными средствами, способными обрабатывать файлы журналов используемого в дискредитируемой системе формата		
127	Угроза подмены действия пользователя путём обмана. Угроза заключается в возможности нарушителя выполнения неправомерных действий в системе от имени другого пользователя с помощью методов социальной инженерии (обмана пользователя, навязывание ложных убеждений) или технических методов (использование прозрачных кнопок, подмена надписей на элементах управления и др.). Данная угроза обусловлена слабостями интерфейса взаимодействия с пользователем или ошибками пользователя. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя прав на проведение нужных от него нарушителю операций	актуально	
128	Угроза подмены доверенного пользователя. Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	охарактеризовать как «имитация действий клиента». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника/получателя информации. Реализация данной угрозы возможна при наличии у нарушителя подключения к вычислительной сети, а также сведений о конфигурации сетевых устройств, типе используемого программного обеспечения и т.п.		
129	Угроза подмены резервной копии программного обеспечения BIOS. Угроза заключается в возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания или создания необходимости выполнения процедуры восстановления предыдущей версии программного обеспечения BIOS/UEFI, предварительно подменённой нарушителем. Данная угроза обусловлена недостаточностью мер разграничения доступа и контроля целостности резервных копий программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в следующих условиях: - нарушитель успешно подменил резервную копию программного обеспечения BIOS/UEFI; - возникла необходимость восстановления предыдущей версии программного обеспечения BIOS/UEFI (данное условие может произойти как случайно, так и быть спровоцировано нарушителем)	не актуально	BIOS защищен паролем; обновление BIOS запрещено
130	Угроза подмены содержимого сетевых ресурсов. Угроза заключается в возможности осуществления нарушителем несанкционирован-	не актуально	у нарушителя отсутствуют права на доступ к сетевым ресурсам

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности содержимого электронного сообщения. Реализация данной угрозы возможна при условии наличия у нарушителя прав на доступ к сетевым ресурсам и отсутствии у пользователя сети мер по обеспечению их целостности		
131	Угроза подмены субъекта сетевого доступа. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения. Данную угрозу можно охарактеризовать как «имитация действий сервера». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника информации. Реализация данной угрозы возможна при условии успешной выдачи себя нарушителем за законного отправителя (например, с помощью ложных фишинговых вебсайтов). Ключевое отличие от «угрозы подмены содержимого сетевых ресурсов» заключается в том, что в данном случае нарушитель не изменяет оригинального содержимого электронного ресурса (вебсайта, электронного письма), а только слу-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	жебные сведения		
132	Угроза получения предварительной информации об объекте защиты. Угроза заключается в возможности раскрытия нарушителем защищаемых сведений о состоянии защищённости дискредитируемой системы, её конфигурации и потенциальных уязвимостях и др., путём проведения мероприятий по сбору и анализу доступной информации о системе. Данная угроза обусловлена наличием уязвимостей в сетевом программном обеспечении, позволяющим получить сведения о конфигурации отдельных программ или системы в целом (отсутствие контроля входных данных, наличие открытых сетевых портов, неправильная настройка политик безопасности и т.п.). Реализация данной угрозы возможна при условии получения информации о дискредитируемой системе с помощью хотя бы одного из следующих способов изучения дискредитируемой системы: - анализ реакций системы на сетевые (в т.ч. синтаксически неверные или нестандартные) запросы к открытым в системе сетевым сервисам, которые могут стать причиной вызова необработанных исключений с подробными сообщениями об ошибках, содержащих защищаемую информацию (о трассировке стека, о конфигурации системы, о маршруте прохождения сетевых пакетов); - анализ реакций системы на строковые URI-запросы (в т.ч. неверные SQL-запросы, альтернативные пути доступа к файлам). Данная угроза отличается от угрозы перехвата данных и других угроз сбора данных тем, что нарушитель активно опрашивает дискредитируемую систему, а не просто за ней наблюдает	актуально	
	1Угроза потери доверия к поставщику об-	не актуально	поставщик облач-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
34	лачных услуг Угроза заключается в возможности снижения уровня защищённости и допущения дополнительных ошибок в обеспечении безопасности защищаемой в облачной системе информации из-за невосполнимого оттока у поставщика облачных услуг необходимых ресурсов в связи с потерей потребителями облачных услуг доверия к их поставщику. Данная угроза обусловлена тем, что из-за обнародования фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, происходит потеря доверия к такому поставщику со стороны потребителей облачных услуг, и, как следствие, возникает необходимость лавинообразного выделения поставщиком облачных услуг ресурсов (человеческих, технических, финансовых) для решения возникающих в данной ситуации задач (множественные консультации пользователей, экстренный пересмотр политик безопасности, модернизация системы защиты и др.), что не только может вызвать нехватку ресурсов для обеспечения текущего уровня защищённости информации, но и спровоцировать допуск «в спешке» новых ошибок. Реализация данной угрозы возможна в случае обнародования единичных или множественных фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, повлёкших значительные убытки для его клиентов		ных услуг обладает высоким финансовым и техническим потенциалом
135	Угроза потери и утечки данных, обрабатываемых в облаке. Угроза заключается в возможности нарушения конфиденциальности, целостности и доступности защищаемой информации потребителей облачных услуг, обрабатываемой в облачной системе. Данная угроза обусловлена слабостями	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	мер защиты информации, обрабатываемой в облачной системе. Реализация данной угрозы возможна в случае допущения поставщиком (некорректный выбор или настройка средств защиты) или потребителем (потеря пароля, электронного ключа, вход с небезопасной консоли) облачных услуг ошибок при обеспечении безопасности защищаемой информации		
137	Угроза потери управления облачными ресурсами Угроза заключается в возможности нарушения договорных обязательств со стороны поставщика облачных услуг в отношении их потребителя из-за значительной сложности построения эффективной системы управления облачными ресурсами облачной системы, особенно использующей облачные ресурсы других поставщиков облачных услуг. Данная угроза обусловлена сложностью определения логического и физического местоположения облачных ресурсов, недостаточностью мер физического контроля доступа к хранилищам данных, резервного копирования и др., а также необходимостью учёта особенностей законодательства в области защиты информации стран, резидентами которых являются поставщики облачных услуг, выполняющих роль субподрядчиков по оказанию заказанных облачных услуг. Реализация данной угрозы возможна при условии, что выполнение требований к функционалу облачной системы затрудняется (или становится невозможным) из-за правовых норм других стран, участвующих в трансграничной передаче облачного трафика	не актуально	не используются трансграничная передача ПДн
138	Угроза потери управления собственной инфраструктурой при переносе её в облако.	не актуально	поставщик облачных услуг реализует мероприятия

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Угроза заключается в возможности допуска ошибок в управлении инфраструктурой системы потребителя облачных услуг, иммигрированной в облако, со стороны поставщика облачных услуг из-за отсутствия у него сведений об особенностях управления конкретной системы, а также из-за отсутствия у потребителя облачных услуг, обладающего такими сведениями, возможности проводить весь комплекс работ по управлению инфраструктурой собственной системы в связи с её иммиграцией в облако. Данная угроза обусловлена невозможностью достоверной оценки потребителем облачных услуг реального уровня защищённости, обеспечиваемого поставщиком облачных услуг в отношении защищаемой информации потребителя облачных услуг, в связи с закрытостью для потребителей сведений о применяемых поставщиком облачных услуг технологиях, программных и технических решениях, а также конкретных параметрах настроек средств защиты информации. Реализация данной угрозы возможна в случаях передачи поставщику облачных услуг части функций управления системой потребителя облачных услуг (при миграции части или всей системы в облако)		по защите информации
139	Угроза преодоления физической защиты. Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной техники системы путём преодоления системы контроля физического доступа, организованной в здании предприятия. Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.).	не актуально	в помещения где обрабатываются персональные данные имеют доступ только доверенные лица

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.)		
140	Угроза приведения системы в состояние «отказ в обслуживании». Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой. Данная угроза обусловлена тем, что для обработки каждого сетевого запроса системой потребляется часть её ресурсов, а также слабостями сетевых технологий, связанными с ограниченностью скорости обработки потоков сетевых запросов, и недостаточностью мер контроля за управлением соединениями. Реализация данной угрозы возможна при условии превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы (таких как способность переносить повышенную нагрузку или приобретать дополнительные ресурсы для предотвращения их исчерпания). Ключевым фактором успешности реализации данной угрозы является число запросов, которое может отправить нарушитель в единицу времени: чем больше это число, тем выше вероятность успешной реализации данной угрозы для дискредитируемой системы	актуально	
141	Угроза привязки к поставщику облачных услуг Угроза заключается в возможности возникновения трудно решаемых (или даже неразрешимых) проблем технического, организационного, юридического или другого характера, препятствующих осуществлению потребителем облачных услуг смены	не актуально	существует возможность смены поставщика облачных услуг

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	их поставщика. Данная угроза обусловлена отсутствием совместимости между форматами данных и программными интерфейсами, используемыми в облачных инфраструктурах различных поставщиков облачных услуг. Реализация данной угрозы возможна при условии использования поставщиком облачных услуг нестандартного программного обеспечения или формата образов виртуальных машин и отсутствием средств преобразования образа виртуальной машины из используемого им формата в другой (используемый другим поставщиком)		
142	Угроза приостановки оказания облачных услуг вследствие технических сбоев Угроза заключается в возможности снижения качества облачных услуг (или даже отказа в их оказании конечным потребителям) из-за возникновения технических сбоев хотя бы у одного из поставщиков облачных услуг (входящих в цепь посредников при оказании облачных услуг их конечному потребителю), а также из-за возникновения существенных задержек или потерь в каналах передачи данных, арендуемых потребителем или поставщиками облачных услуг. Данная угроза обусловлена слабостями процедуры контроля за выполнением технического обслуживания и соблюдением режимов функционирования технических средств облачной информационной системы. Реализация данной угрозы возможна при условии отсутствия механизмов резервирования средств обработки, хранения и передачи информации, входящих в состав облачной информационной системы	не актуально	реализуется резервирование средств обработки, хранения и передачи информации, входящих в состав облачной информационной системы
143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.	не актуально	у нарушителя отсутствуют права на отправку команды или специ-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Угроза заключается в возможности прерывания нарушителем технологии обработки информации в дискредитируемой системе путём осуществления деструктивного программного (локально или удалённо) воздействия на средства хранения (внешних, съёмных и внутренних накопителей), обработки (процессора, контроллера устройств и т.п.) и (или) ввода/вывода/передачи информации (клавиатуры и др.), в результате которого объект защиты перейдёт в состояние «отказ в обслуживании». При этом вывод его из этого состояния может быть невозможен путём простой перезагрузки системы, а потребует проведения ремонтно-восстановительных работ. Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации		ально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации
144	Угроза программного сброса пароля BIOS. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера путём ввода «пустого» пароля. Данная угроза обусловлена слабостями мер разграничения доступа в операционной системе к функции сброса пароля BIOS/UEFI. Реализация данной угрозы возможна при условиях: - наличия в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля непосредственно из-под операционной системы; - наличия у нарушителя специальных программных средств, реализующих сброс па-	не актуально	у нарушителя отсутствуют привилегии на установку программного обеспечения

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	роля, а также прав в операционной системе для установки и запуска данных средств		
145	Угроза пропуска проверки целостности программного обеспечения. Угроза заключается в возможности внедрения нарушителем в дискредитируемую систему вредоносного программного обеспечения путём обманного перенаправления запросов пользователя или его программ на собственный сетевой ресурс, содержащий вредоносное программное обеспечение, для его «ручной» или «автоматической» загрузки с последующей установкой в дискредитируемую систему от имени пользователя или его программ. Данная угроза обусловлена слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения. Реализация данной угрозы возможна при условии успешного использования обманных техник одного из следующих методов: - «ручного метода» – нарушитель, используя обманные механизмы, убеждает пользователя перейти по ссылке на сетевой ресурс нарушителя, что приводит к запуску вредоносного кода на компьютере пользователя, или убеждает пользователя самостоятельно загрузить и установить вредоносную программу (например, под видом игры или антивирусного средства); - «автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер	актуально	
149	Угроза сбоя обработки специальным образом изменённых файлов. Угроза заключается в возможности осуществления нарушителем различных неправомерных действий от имени дискредити-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	рованных приложений путём вызова сбоя в их работе за счёт внесения изменений в обрабатываемые дискредитируемыми программами файлы или их метаданные. Данная угроза обусловлена слабостями механизма проверки целостности обрабатываемых файлов и корректности, содержащихся в них данных. Реализация данной угрозы возможна в условиях: - наличия у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке; - успешно созданном в дискредитируемой системе механизме перехвата управления над обработкой нарушителем программного сбоя		
150	Угроза сбоя процесса обновления BIOS. Угроза заключается в возможности выведения из строя компьютера из-за внесения критических ошибок в программное обеспечение BIOS/UEFI в результате нарушения процесса его обновления. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера как при установке корректной/совместимой версии обновления (из-за сбоев, помех и т.п.), так и при установке повреждённой/несовместимой версии обновления (из-за отсутствия механизма проверки целостности и совместимости)	не актуально	обновление BIOS запрещено; ремонт и обслуживание компьютеров осуществляется специалистами организации
151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL. Угроза заключается в возможности получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уяз-	не актуально	у нарушителя отсутствует доступ к исследуемому сетевому ресурсу

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	вимостей путём исследования WSDL-интерфейса веб-сервера. Данная угроза обусловлена недостаточностью мер по обеспечению конфиденциальности информации, реализованных в WSDL-сервисах, предоставляющих подробные сведения о портах, службах и соединениях, доступных пользователям. Реализация данной угрозы возможна при наличии у нарушителя сетевого доступа к исследуемому сетевому ресурсу и специальных программных средств сканирования сети		
152	Угроза удаления аутентификационной информации. Угроза заключается в возможности отказа легитимным пользователям в доступе к информационным ресурсам, а также в возможности получения нарушителем привилегий дискредитированного пользователя за счёт сброса (обнуления, удаления) его аутентификационной информации. Данная угроза обусловлена слабостями политики разграничения доступа к аутентификационной информации и средствам работы с учётными записями пользователей. Реализация данной угрозы возможна при выполнении одного из следующих условий: - штатные средства работы с учётными записями пользователей обладают функционалом сброса аутентификационной информации, и нарушитель получил привилегии в дискредитируемой системе на использование данных средств; - нарушитель обладает специальным программным обеспечением, реализующим функцию сброса аутентификационной информации, и получил привилегии в дискредитируемой системе на использование данных средств	не актуально	у нарушителя отсутствуют привилегии на сброс аутентификационной информации
153	Угроза усиления воздействия на вычисли-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	тельные ресурсы пользователей при помощи сторонних серверов. Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на дискредитируемую систему большим объёмом сетевого трафика, генерируемого сторонними серверами в ответ на сетевые запросы нарушителя, сформированные от имени дискредитируемой системы. Генерируемый сторонними серверами сетевой трафик значительно превышает объём сетевых запросов, формируемых нарушителем. Данная угроза обусловлена слабостями мер межсетевого экранирования дискредитируемой информационной системы, мер контроля подлинности сетевых запросов на сторонних серверах, а также слабостями модели взаимодействия открытых систем. Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о сторонних серверах с недостаточными мерами контроля подлинности сетевых запросов; - сведений о сетевом адресе дискредитируемой системы; - специального программного обеспечения, реализующего функции генерации сетевых пакетов		
154	Угроза установки уязвимых версий обновления программного обеспечения BIOS. Угроза заключается в возможности внесения уязвимостей в программное обеспечение BIOS/UEFI в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации BIOS/UEFI или выполнения вредоносного кода при каждом запуске компьютера. Данная угроза обусловлена слабостями	не актуально	обновление BIOS запрещено; ремонт и обслуживание компьютеров осуществляется специалистами организации

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	мер контроля отсутствия уязвимостей в только что вышедших версиях обновления программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера		
155	Угроза утраты вычислительных ресурсов. Угроза заключается в возможности отказа легитимному пользователю в выделении ресурсов для обработки его запросов из-за исчерпания нарушителем свободных ресурсов в системе, осуществлённого путём их несанкционированного исключения из общего пула ресурсов на основе техник «утечки ресурсов» или «выделения ресурсов». Данная угроза обусловлена слабостями механизма контроля за распределением вычислительных ресурсов между пользователями, а также мер межсетевого экранирования дискредитируемой информационной системы и контроля подлинности сетевых запросов на сторонних серверах. Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы; - привилегий, достаточных для осуществления деструктивных воздействий («утечки» или «выделения») в дискредитируемой системе; - отсутствие у администраторов возможности: для техники «утечки ресурсов» – перезагрузки системы во время отправки нарушителем большого числа запросов на выделение ресурсов, а для техники «выделения ресурсов» – форсированного освобождения ресурсов, выделенных по запросам вредоносных процессов	актуально	
156	Угроза утраты носителей информации.	не актуально	осуществляется

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Угроза заключается в возможности раскрытия информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или её потери (в случае отсутствия резервной копий данных). Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников		учет носителей информации; осуществляется резервирования защищаемых данных
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации. Угроза заключается в возможности умышленного выведения из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода / вывода / передачи информации. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	не актуально	в помещения где обрабатываются персональные данные имеют доступ только доверенные лица
158	Угроза форматирования носителей информации. Угроза заключается в возможности утраты хранящейся на форматируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации.	не актуально	осуществляется резервирования защищаемых данных

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	Данная угроза обусловлена слабостью мер ограничения доступа к системной функции форматирования носителей информации. На реализацию данной угрозы влияют такие факторы как: - время, прошедшего после форматирования; - тип носителя информации; - тип файловой системы носителя; - интенсивность взаимодействия с носителем после форматирования и др.		
159	Угроза «форсированного веб-браузинга». Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	не актуально	доступ к информационным ресурсам имеют только доверенные лица
160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации. Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации. Данная угроза обусловлена слабостями	не актуально	в помещения где обрабатываются персональные данные имеют доступ только доверенные лица

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	мер контроля физического доступа к средствам хранения, обработки и (или) ввода / вывода / передачи информации. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)		
162	Угроза эксплуатации цифровой подписи программного кода. Угроза заключается в возможности повышения нарушителем привилегий в системах, использующих цифровую подпись кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма подписывания программного кода. Данная угроза обусловлена слабостями в механизме подписывания программного кода. Реализация данной угрозы возможна при следующих условиях: - дискредитируемый программный код написан с помощью фреймворка (framework), поддерживающего подписывание программного кода; - дискредитируемый программный код подписан вендором (поставщиком программного обеспечения); - нарушитель имеет возможность внедрить программный код в дискредитируемый компьютер	не актуально	механизм подписывания программного кода не используется
163	Угроза перехвата исключения/сигнала из привилегированного блока функций. Угроза заключается в возможности нарушителя получить права на доступ к защищаемой информации путём перехвата исключений/сигналов, сгенерированных участком программного кода, исполняемого с повышенными привилегиями (приви-	не актуально	язык программирования, поддерживающий механизм привилегированных блоков не используется

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	легированным блоком функций) и содержащего команды по управлению защищаемой информацией. Данная угроза обусловлена тем, что вызов программных функций в привилегированном режиме подразумевает отключение для них механизмов разграничения доступа. Реализация данной угрозы возможна при следующих условиях: - дискредитируемая программа, написана на языке программирования, поддерживающего механизм привилегированных блоков (например, Java); - в дискредитируемой программе вызов привилегированных блоков осуществлён небезопасным способом (использовано публичное объявление внутренних функций, использована генерация исключений из привилегированного блока); - нарушитель обладает правами, достаточными для перехвата программных исключений в системе		
164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре Угроза заключается в возможности распространения негативных последствий от реализации угроз на физическом или виртуальном уровне облачной инфраструктуры на уровни управления и оркестровки, а также на все информационные системы, развёрнутые на базе дискредитированной облачной инфраструктуры. Данная угроза обусловлена невозможностью функционирования информационных систем в облаке при некорректной работе самой облачной инфраструктуры, а также зависимостью работоспособности верхних уровней облачной инфраструктуры от работоспособности нижних. Реализация данной угрозы возможна в случае приведения облачной инфраструктуры на физическом или виртуальном	не актуально	поставщик облачных услуг реализует мероприятия по защите информации

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	уровне облачной инфраструктуры в состояние «отказ в обслуживании»		
165	Угроза включения в проект не достоверно испытанных компонентов. Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии выбора для применения в системе компонентов по цене, разрекламированности и др.	не актуально	осуществляется контроль за проектированием систем, связанных с безопасностью
166	Угроза внедрения системной избыточности. Угроза заключается в возможности снижения скорости обработки данных (т.е. доступности) компонентами программного обеспечения (или системы в целом) из-за внедрения в него (в неё) избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект). Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии внесения изменений в перечень задач, решаемых проектируемым программным обеспечением (проектируемой системой)	не актуально	используются только необходимые компоненты программного обеспечения
167	Угроза заражения компьютера при посещении неблагонадёжных сайтов. Угроза заключается в возможности нару-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	шения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадёжным содержимым и запускаемыми с привилегиями дискредитированных пользователей. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадёжным содержимым		
168	Угроза «кражи» учётной записи доступа к сетевым сервисам. Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путём получения информации идентификации / аутентификации, соответствующей учётной записи доступа пользователя к сетевым сервисам (социальной сети, облачным сервисам и др.), с которой связан неактивный/несуществующий адрес электронной почты. Данная угроза обусловлена недостаточностью мер контроля за активностью/существованием ящиков электронной почты. Реализация данной угрозы возможна при условиях: - наличия статуса «свободен для занимания» у адреса электронной почты, с которым связана учётная запись доступа пользователя к сетевым сервисам (например, если пользователь указал при регистрации несуществующий адрес или долго не обращался к почтовому ящику, вследствие чего, его отключили); - наличия у нарушителя сведений об адресе электронной почты, с которым связана учётная запись дискредитируемого пользо-	не актуально	информация идентификации/аутентификации не связана с адресом электронной почты

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	вателя для доступа к сетевым сервисам		
169	Угроза наличия механизмов разработчика. Угроза заключается в возможности перехвата управления программой за счёт использования отладочных механизмов (специальных программных функций или аппаратных элементов, помогающих проводить тестирование и отладку средств во время их разработки). Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе разработки средств защиты информации. Реализация данной угрозы возможна при условии, что в программе не удалены отладочные механизмы	не актуально	отладочные механизмы не используются
170	Угроза неправомерного шифрования информации. Угроза заключается в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа. Данная угроза обусловлена наличием слабостей в антивирусной защите, а также в механизмах разграничения доступа. Реализация данной угрозы возможна при условии успешной установки нарушителем на дискредитируемый компьютер средства криптографического преобразования информации, а также успешного обнаружения (идентификации) нарушителем защищаемых файлов	актуально	
171	Угроза скрытного включения вычислительного устройства в состав бот-сети. Угроза заключается в возможности опосредованного осуществления нарушителем деструктивного воздействия на информационные системы с множества вычислительных устройств (компьютеров, мобильных технических средств и др.), подклю-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	чённых к сети Интернет, за счёт захвата управления такими устройствам путём несанкционированной установки на них: - вредоносного ПО типа Backdoor для обеспечения нарушителя возможностью удалённого доступа/управления дискредитируемым вычислительным устройством; - клиентского ПО для включения в ботнет и использования созданного таким образом ботнета в различных противоправных целях (рассылка спама, проведение атак типа «отказ в обслуживании» и др.). Данная угроза обусловлена уязвимостями в сетевом программном обеспечении и слабостями механизмов антивирусного контроля и межсетевого экранирования. Реализация данной угрозы возможна при условии наличия выхода с дискредитируемого вычислительного устройства в сеть Интернет		
172	Угроза распространения «почтовых червей». Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа «почтовый червь», а также невольного участия в дальнейшем противоправном распространении вредоносного кода. Данная угроза обусловлена слабостями механизмов антивирусного контроля. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя электронного почтового ящика, а также наличия в его адресной книге хотя бы одного адреса другого пользователя	актуально	
173	Угроза «спама» веб-сервера. Угроза заключается в возможности непра-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	вомерного осуществления нарушителем массовой рассылки коммерческих, политических, мошеннических и иных сообщений на веб-сервер без запроса со стороны дискредитируемых веб-серверов. Данная угроза обусловлена уязвимостями механизмов фильтрации сообщений, поступающих из сети Интернет. Реализация данной угрозы возможна при условии наличия в дискредитируемом веб-сервере активированного функционала, реализующего различные почтовые сервера, службы доставки мгновенных сообщений, блоги, форумы, аукционы веб-магазинов, онлайн-сервисы отправки SMS-сообщений, онлайн-сервисы голосования и др.		
174	Угроза «фарминга». Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации / аутентификации) пользователя путём скрытного перенаправления пользователя на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию. Данная угроза обусловлена уязвимостями DNS-сервера, маршрутизатора. Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; - средств создания и запуска поддельного сайта; - специальных программных средств типа «эксплойт», реализующих перенаправление пользователя на поддельный сайт. Кроме того, угрозе данного типа подвержены подлинные сайты, не требующие установления безопасного соединения перед вводом информации ограниченного доступа	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
175	Угроза «фишинга». Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации / аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть заражённое вложение в письме. Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах «фишинга». Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; - средств создания и запуска поддельного сайта; - сведений о контактах пользователя с доверенной организацией (номер телефона, адрес электронной почты и др.). Для убеждения пользователя раскрыть информацию ограниченного доступа (или открыть вложение в письмо) наиболее часто используются поддельные письма от администрации какой-либо организации, с которой взаимодействует пользователь (например, банк)	актуально	
176	Угроза нарушения технологического / производственного процесса из-за временных задержек, вносимых средством защиты. Угроза заключается в возможности приведения системы в состояние «отказ в об-	не актуально	система защиты информации сбалансирована

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	служивании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации средствами защиты информации, вызванной необходимостью обработки передаваемой / обрабатываемой информации на предмет выявления и нейтрализации угроз безопасности информации. На реализацию данной угрозы влияет не только номенклатура применяемых средств защиты информации, параметры их настройки, объём передаваемой /обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются средствами защиты информации		
177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью. Угроза заключается в возможности возникновения ошибок в работе системы вследствие отсутствия (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора, средства учёта нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.). Реализуемость данной угрозы зависит от требований, предъявляемых к процедурам обнаружения и исправления ошибок во вводимых данных в систему, связанную с безопасностью, а также разницей между	не актуально	оператор не управляет системой, связанной с безопасностью

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	этими требованиями и фактическим уровнем обнаружения и исправления ошибок		
178	Угроза несанкционированного использования системных и сетевых утилит. Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему за счёт использования имеющихся или предварительно внедрённых стандартных (известных и обычно не определяемых антивирусными программами как вредоносных) системных и сетевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети). Реализация данной угрозы возможна при условиях: - наличие в системе стандартных системных и сетевых утилит или успешное их внедрение нарушителем в систему и сокрытие (с использованием существующих архивов, атрибутов «скрытый» или «только для чтения» и др.); - наличие у нарушителя привилегий на запуск таких утилит	не актуально	нарушитель не обладает привилегиями на запуск сетевых утилит
179	Угроза несанкционированной модификации защищаемой информации. Угроза заключается в возможности нарушения целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём. Реализация данной угрозы возможна в случае получения нарушителем системных прав на запись данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздей-	актуально	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	ствия		
180	Угроза отказа подсистемы обеспечения температурного режима. Угроза заключается в возможности повреждения части компонентов системы или системы в целом вследствие выхода температурного режима их работы из заданных требований из-за возникновения отказа входящих в неё подсистем вентиляции и температурных приборов. Реализация данной угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на удалённое отключение / вывод из строя компонентов подсистемы обеспечения температурного режима	не актуально	используются системы мониторинга температуры
181	Угроза перехвата одноразовых паролей в режиме реального времени. Угроза заключается в возможности получения нарушителем управления критическими операциями пользователя путём перехвата одноразовых паролей, высылаемых системой автоматически, и использования их для осуществления неправомерных действий до того, как истечёт их срок действия (обычно, не более 5 минут). Реализация данной угрозы возможна при выполнении следующих условий: - наличие у нарушителя сведений об информации идентификации / аутентификации дискредитируемого пользователя условно-постоянного действия; - успешное осуществление нарушителем перехвата трафика между системой и пользователем	не актуально	одноразовые пароли не используются
182	Угроза физического устаревания аппаратных компонентов. Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отка-	не актуально	используется современные аппаратные компоненты

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	зов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций). Возможность реализации данной угрозы возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем		

3. Актуальные угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы безопасности Российской Федерации

№	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования	да
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	нет
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	нет

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	проведение атаки при нахождении в пределах контролируемой зоны	актуально	
1.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ	не актуально	- проводятся работы по подбору персонала; - доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; - документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; - помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; - утвержден перечень лиц, имеющих право доступа в помещения
1.3	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся	не актуально	- проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДн, обеспечивается в соответствии с контрольно-пропускным режимом; - сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; - сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	СВТ, на которых реализованы СКЗИ и СФ		
1.4	использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	- проводятся работы по подбору персонала; - помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; - сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; - в ИСПДн используются сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты
2.1	физический доступ к СВТ, на которых реализованы СКЗИ и СФ	не актуально	- проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается по-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			стоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода
2.2	возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	- проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации
3.1	создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	не актуально	- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности; - проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где распо-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			лагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; - осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей; - на АРМ и серверах, на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты
3.2	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в	не актуально	- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реа-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		лизации возможности; - высокая стоимость и сложность подготовки реализации возможности
3.3	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	не актуально	- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	не актуально	- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности; - проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			- представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; -осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей; - на АРМ и серверах, на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты
4.2	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	не актуально	- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	возможность воздействовать на любые компоненты СКЗИ и СФ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности